

基于鲁棒图像水印的文本信息加密技术

孙秋冬 马文新 颜文英 戴虹

(上海第二工业大学电子与电气工程学院, 上海 201209)

摘要 通过利用一个新视觉模型计算图像分块的临界噪声阈值矩阵 JND 阵, 提出了一个基于分块 DWT 的图像自适应公开水印技术的文本信息加密算法。该算法以一个文本文件为水印, 先对文本文件进行 Reed-Solomon 纠错编码, 再转换为二值序列作为水印, 并进行随机置乱。然后在原图像 8×8 分块的 Hilbert 扫描序列中选取两相邻块分别进行一层 DWT, 再根据各分块 JND 阈值, 不同强度地调整两相邻块各对应细节子带均值之间的大小关系以自适应地嵌入水印。实验结果表明, 即使在较低的峰值信噪比下嵌入水印也具有很好的透明性, 同时, 该算法对 16 种常见图像攻击有较高的鲁棒性, 特别是信号增强操作处理几乎不影响加密信息的正确提取。

关键词 RS 纠错编码 随机置乱 人类视觉系统 Hilbert 扫描 离散小波变换 公开水印技术 文本加密
中图法分类号: TP309.7, TP751.1 **文献标识码**: A **文章编号**: 1006-8961(2008)10-1942-05

Text Encryption Technique Based on Robust Image Watermarking

SUN Qiu-dong, MA Wen-xin, YAN Wen-ying, DAI Hong

(School of Electronic and Electrical Engineering, Shanghai Second Polytechnic University, Shanghai 201209)

Abstract The JND (just noticed difference) threshold matrix based on block was calculated by a new human visual model, and then a text encryption algorithm based on image-adaptive public watermarking technique operating in DWT domain was presented. Firstly, the text in a file was encoded with Reed-Solomon codes for robust and transferred into a binary sequence, which could be permuted randomly to a final watermark. Then, two neighboring blocks were selected from the Hilbert scanning sequence of the host image blocks in turn, and transformed by 1-level DWT. By JND, the final watermark was embedded into the host image by modifying the average values of the two corresponding subbands. The experimental results show that the embedded watermark is invisible to human eyes at a low PSNR, and the algorithm is robust to common image processing operations, especially to signal enhancement. The conclusion is that the algorithm is effective and practical.

Keywords Reed-Solomon code, random scrambling, HVS, Hilbert scanning, DWT, public watermarking technique, text encryption

1 引言

多年来,人们对多媒体信息传输的安全问题做了大量工作,发展了置乱技术、水印技术、分存技术和隐藏技术。一个有效的数字水印技术必须

具备透明性、鲁棒性、安全性等基本特征,而前两者是一对矛盾,化解矛盾的有效途径之一就是充分利用人类视觉系统(human visual system, HVS)的屏蔽特性^[1]。由于小波变换良好的时-空局部特性具有与 HVS 屏蔽特性极其相符的变换机制,因而使得 DWT (discrete wavelet transformation) 域水

基金项目:上海市教育委员会重点学科基金项目(J51801);上海市教育委员会科学发展基金项目(06RZ012)

收稿日期:2008-07-11;**改回日期**:2008-07-31

第一作者简介:孙秋冬(1963 ~),男,副教授。1988 年于上海科学技术大学获硕士学位。主要研究方向为电子技术、信息处理和软件工程。E-mail:qdsun@ee.ssp.cn

印算法具有广阔的前景^[2]。用于信息隐藏的数字水印技术还必须做到长文本信息的嵌入和盲水印提取。

过去几年中,产生了很多运用 HVS 和 DWT 技术的水印算法^[1~4],有些算法^[1~3]也实现了盲水印提取,但这些算法大多是针对二值图像的水印,这些算法都不适合用于文本信息的保密通信。到目前,也很少见用水印技术直接进行文本信息加密的算法。

本文充分利用 HVS 的屏蔽特性,给出一种改进的定量噪声临界阈值 JND (just noticed difference) 计算方法,并结合 RS (reed-solomon) 纠错编码、冗余编码、置乱技术和 Hilbert 扫描技术,提出一种基于分块 DWT 的图像自适应公开水印技术的文本信息加密算法,为文本信息以水印方式实现保密通信进行有益的探索。

2 视觉特性和块视觉阈值 JND 计算

2.1 人眼视觉特性

实验表明,人眼观察到的主观亮度并不完全由物体本身的亮度所决定,它还与背景亮度有关。实验测得的人眼分辨力曲线如图 1 所示^[5]。其中的图 1(a)是无背景情况,图 1(b)为有背景情况,图中 ΔB 为物体局部亮度的变化量, $\Delta B/B$ 为 Weber 比。

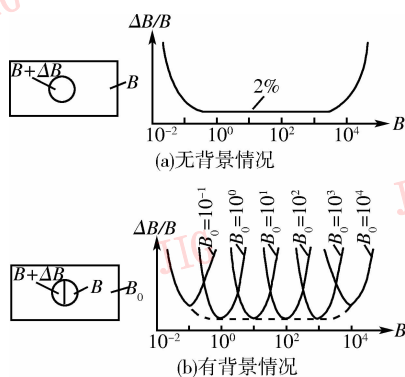


图 1 人眼分辨力曲线

Fig. 1 Visual resolution curve

在数字图像中,图像的灰度 f 反映了物体的亮度 B ,因此,在某个背景灰度 f 下,人眼能分辨的灰度相对变化率 $\gamma(f) = \Delta f/f$ 与该背景灰度 f 也为一种非线性关系,一般采用二次曲线来近似^[1,3,4]。文献^[5]经大量实验后,认为采用式(1)的指数曲线来近似更适合和灵活。

$$\gamma(f) = \frac{\Delta f}{f} = \alpha \left[\frac{1}{k_1} e^{\frac{1}{s_1 f}} + \frac{1}{k_2} e^{\frac{1}{s_2 (256-f)}} \right] \quad (1)$$

式中, α 为人眼分辨力常数,其值一般可取 0.02, e 为自然数的底,系数 k_1, k_2, s_1 和 s_2 于调节人眼对物体边缘或纹理在高、低亮度背景下的敏感性,一般可选 $k_1 = e, k_2 = e^{\frac{1}{128}}, s_1 = \frac{1}{128}, s_2 = 1$ 。

2.2 块视觉阈值 JND 计算

利用块 JND 来调节水印嵌入强度能保证水印同时具有良好的透明性和鲁棒性,计算时主要考虑:

(1) 人眼对不同背景灰度 f 下的噪声的掩盖因子与 Δf 成正比,即

$$S(u, v) = \beta \Delta f = \beta \gamma(f) = \beta \gamma(A) A \quad (2)$$

式中, β 为调节因子。实验中,用 8×8 图像块 $B(u, v)$ 代表一个亮度区域,该块的灰度平均值 $A = \text{mean}(B(u, v))$ 近似作为其背景灰度 f 。

(2) 人眼对纹理的掩盖效应因子用归一化熵值来表示^[2,4]。若设 $E'(u, v)$ 为块 $B(u, v)$ 的熵值,归一化区间为 $[a, b]$,则纹理掩盖效应因子为

$$E(u, v) = (b - a) \frac{E'(u, v) - \min(E')}{\max(E') - \min(E')} + a \quad (3)$$

综上,图像分块的可容许噪声阈值可表示为

$$T'(u, v) = S(u, v) E(u, v) \quad (4)$$

为了保证水印嵌入强度的可控性和不可见性,将式(4)归一化到区间 $[c, d]$,得

$$T(u, v) = (d - c) \frac{T'(u, v) - \min(T')}{\max(T') - \min(T')} + c \quad (5)$$

(3) 2 维数字图像经一层小波变换后得到 4 个子图像 LL, LH, HL, HH 。人眼对不同方向不同层次的高频子带图像的噪声不是非常敏感^[4]。设不同层 l 不同方向 s 子带对噪声的掩盖因子为 $F(l, s)$,则

$$F(l, s) = F(l) \times F(s) \quad (6)$$

其中

$$F(l) = \{1, 0.32, 0.16, 0.1\} \quad l = 0, 1, 2, 3 \quad (7)$$

$$F(s) = \begin{cases} \sqrt{2} & s \in HH \\ 1 & \text{其他} \end{cases} \quad (8)$$

综上,图像分块 $B(u, v)$ 经一层小波变换后各细节子带 $D_{u,v}^{l,s}$ 的视觉可容许临界噪声阈值可表示为

$$J(u, v, l, s) = T(u, v) F(l, s) \quad (9)$$

3 图像小波域的文本信息加密算法

3.1 加密算法

(1) 读入密文文本文件, 将文本的内码用 8 位整数序列保存。

(2) 为了增强系统的鲁棒性, 有必要对文本内码进行纠错编码。由于 RS 码具有很强的纠错能力, 故可对文本内码在 $GF(2^8)$ 域中进行 (16, 8) RS 编码, 得到编码后的文本内码。虽然码长增加一倍, 但能实现 4 个内码的纠错功能。

(3) 将文本内码按位从高位到低位转换为 1 维向量并适当添零, 使其长度 L 的整数倍正好为明文图像块数的 1.5 倍, 得原始的二值水印 W 。

(4) 为了增强算法的鲁棒性, 对水印进行循环位扩展来增加水印的冗余度, 得扩位后的水印 W_{ex} :

$$W_{ex}(n \cdot L + m) = W(m) \quad (10)$$

$$m = 0, 1, \dots, L - 1; n = 0, 1, \dots, Cr - 1$$

式中, Cr 为扩展因子, 对于一幅大小为 $M \times N$ 的 8 位灰度图像 I , 则 8×8 分块数 $N_b = M \times N / 64$, $Cr = 1.5 \times N_b / L$, W_{ex} 的长度为 $L_{ex} = 1.5 N_b$ 。纠错编码增加了文本内码的长度, 会降低水印的冗余度, 故需综合考虑。

(5) 为了增强水印系统的安全性, 对 W_{ex} 进行伪随机置乱。选择一个种子 $seed$, 用伪随机序列产生器产生一个水印源位置随机序列 R_s , $R_s = \{R_s(k) | R_s(k) \in (0, L_{ex} - 1), k = 0, 2, \dots, L_{ex} - 1\}$; 接着在指定位置 pos 开始从 R_s 中循环选择第一个与 $seed$ 不同的值作为种子, 产生另一大小和数值范围与 R_s 一样的目的位置随机序列 R_d 。随机置乱的元素交换规则为

$$W_{ex}(R_d(k)) \leftrightarrow W_{ex}(R_s(k)) \quad (11)$$

$$k = 0, 1, \dots, L_{ex} - 1$$

这一步也可选。

(6) 为了保持图像空间局部相关性, 先对原图像 I 的 8×8 分块按 Hilbert 扫描, 得到原图像分块的行列坐标的两个 Hilbert 索引序列 H_u 和 H_v ,

$$H_u = \left\{ H_u(\tau) | 0 \leq H_u(\tau) \leq \frac{M}{8} - 1, \tau = 0, 1, \dots, N_b - 1 \right\}$$

$$H_v = \left\{ H_v(\tau) | 0 \leq H_v(\tau) \leq \frac{N}{8} - 1, \tau = 0, 1, \dots, N_b - 1 \right\}$$

(7) 水印嵌入^[2]。依次从 Hilbert 索引序列中选出两相邻 8×8 块 $B(H_u(\tau), H_v(\tau))$ 和 $B(H_u(\tau + 1),$

$H_v(\tau + 1))$, 分别记为 B_{uv1} 和 B_{uv2} , 对它们分别作一层 DWT; 最后, 每次在选定的两相邻块 B_{uv1} 和 B_{uv2} 各自细节子带中各选取一对对应子带 $D_{u_1, v_1}^{l, s}$ 和 $D_{u_2, v_2}^{l, s}$ (以下简称 D_1 和 D_2 , 通称 $D_t, t \in \{1, 2\}$, 下同)。设用小波系数来表征细节子带各像素位可容许失真的强度因子,

$$\lambda_t(i, j) = \frac{|D_t(i, j)| + \delta}{\text{mean}(|D_t|) + \delta} \quad (12)$$

$$t \in \{1, 2\}; i, j = 0, 1, \dots, \frac{8}{2^{l+1}}$$

式中, δ 是一个为了防止分母为 0 的很小正数。分别令两相邻块对应小波系数细节子带的临界噪声阈值均值、系数均值差和系数调整量为

$$\mu = \frac{J(u_1, v_1, l, s) + J(u_2, v_2, l, s)}{2} \quad (13)$$

$$dif = (-1)^{W_{ex}(k)} [\text{mean}(D_2) - \text{mean}(D_1)] \quad (14)$$

$$\varepsilon_t(i, j) = (-1)^t \lambda_t(i, j) \frac{\mu - dif}{2} \quad (15)$$

则用下列细节子带小波系数调整方法作为水印嵌入的规则:

$$D'_t(i, j) = \begin{cases} D_t(i, j) - \varepsilon_t(i, j) & dif < \mu \\ D_t(i, j) & \text{其他} \end{cases} \quad (16)$$

(8) 对所有经过系数调整后的子块进行一层 DWT 反变换, 即得到嵌入水印图像 I' 。本次文本加密的密钥为 $Key(Cr, seed, pos)$ 。

3.2 解密算法

文本信息解密是加密的逆过程:

(1) 水印提取^[2]。与水印嵌入时一样通过 Hilbert 扫描含水水印图像 I' 确定两相邻块 B_{uv1} 和 B_{uv2} , 以及其对应的一层 DWT 细节子带 $\hat{D}_1$ 和 $\hat{D}_2$, 则可由下式提取出 Cr 个版本的水印信号:

$$\hat{W}_{ex}(k) = \begin{cases} 1 & \text{mean}(\hat{D}_1) \geq \text{mean}(\hat{D}_2) \\ 0 & \text{其他} \end{cases} \quad (17)$$

(2) 若水印嵌入时进行了随机置乱, 则需根据密钥 Key 产生两组位置交换的伪随机序列, 仍按式 (11) 进行置乱, 从而达到去乱的目的。

(3) 从 Cr 个水印版本中提取出一个最后版本的二值水印:

$$\hat{W}(m) = \begin{cases} 1 & \sum_{n=0}^{Cr-1} \hat{W}_{ex}(n \cdot L + m) \geq \frac{Cr}{2} \\ 0 & \text{其他} \end{cases} \quad (18)$$

(4) 将 1 维二值水印 $\hat{W}$ 转换为文本内码。

(5) 若加密时对文本内码用了 RS 纠错编码, 则

此时需要解码。

(6)将文本内码写入文本文件,完成解密。

4 实验结果及性能分析

算法用 MATLAB 仿真,以一幅 $512 \times 512 \times 8$ 的 Lena 灰度图像作明文,待加密文本分“单行短文”、“多行短文”和“多行长文”来测试。式(1)中的诸参数取其一般值,其余式中 β 取值为1, a 和 b , c 和 d 均分别取值为1和2, δ 取值为0.000 01。实验结果如图2所示。攻击实验除 JPEG 有损压缩和中心区域的剪切用 MATLAB 编程实现外,都是用 Photoshop6.0 完成的。



图 2 Lena 图像经文本加密后的结果

Fig. 2 Result of Lena image after text encrypting

从图2可知,由于充分利用了人眼 HVS 的掩蔽效应,即使在 $PSNR = 23.4\text{dB}$ 较差的情况下,本加密算法也有很好的不可见性。

表1给出了本算法对抗各种攻击的测试结果,符号“√”代表算法完全抗攻击,“×”代表算法对攻击敏感。从表中的数据可知,算法对裁剪、锐化、边缘锐化、对比度增强、亮度增强、高斯噪声、均匀噪声、JPEG 压缩有较强的抗攻击能力;在加密文本较短时,由于水印的冗余度明显增加,算法抗各种攻击的能力也明显增强,此时算法对直方图均衡、运动模糊、椒盐噪声、图像缩放、挤压、旋转扭曲、垂直移位和水平移位也有了较强的抗攻击能力,特别是当加密文本仅有4个字时,算法的抗挤压和旋转扭曲的能力超强。由于加密文本较短时,水印的冗余度成为算法鲁棒性的重要因素,RS 纠错编码和水印的随机置乱对算法的鲁棒性几乎没有影响,因此,为了提高算法的时效,可以取消 RS 纠错编码;当加密文本较长时,水印的冗余度减少,RS 纠错编码成为算法鲁棒性的重要因素,此时算法在有 RS 时的抗攻击性能明显比无 RS 时强,因此,对长文本的加密必需 RS 纠错编码。

表 1 峰值信噪比和抗攻击测试(零误码率)

Tab.1 PSNR and attack defense tests (zero bit error rate)

各种情形的 PSNR 和抗 攻击测试	单行短文(4个中文字)				多行短文(3行12字)				多行长文(192个字)			
	无 RS		有 RS		无 RS		有 RS		无 RS		有 RS	
	无置乱	有置乱	无置乱	有置乱	无置乱	有置乱	无置乱	有置乱	无置乱	有置乱	无置乱	有置乱
PSNR(dB)	32.2	24.7	32.0	24.9	28.4	25.7	29.9	25.9	26.3	23.4	36.6	40.4
JPEG 压缩(%)	81	83	84	82	90	93	90	91	97	97	97	96
裁剪(中心方块)	334	331	317	310	326	285	251	251	10	70	25	93
锐化(次)	>10	>10	>10	>10	>10	>10	>10	>10	0	1	0	1
边缘锐化(次)	>10	>10	>10	>10	>10	>10	>10	>10	1	2	0	1
直方图均衡	√	√	√	√	√	√	√	√	×	×	×	×
对比度增强(%)	79	81	84	81	71	71	67	58	19	32	27	35
亮度增强(%)	>100	>100	>100	>100	>100	>100	>100	>100	22	68	33	44
运动模糊(像素)	14	11	13	9	1	×	4	×	×	×	×	×
高斯噪声(%)	6.4	6.4	6	5.6	2.5	2.1	3.3	3	0.5	0.5	0.5	0.5
均匀噪声(%)	13.7	13.8	13.7	12.7	4.6	3.8	5.9	4.9	0.5	0.9	0.5	0.9
椒盐噪声(%)	7	3	5	3	1	×	1	×	×	×	×	×
缩小放大(最小)	449	458	453	444	490	503	489	489	×	×	×	×
挤压(%)	99	98	100	99	2	1	1	1	×	×	×	×
旋转扭曲(度)	>360	271	312	289	5	2	2	1	×	×	×	×
垂直移位(像素)	2	2	2	2	2	2	2	2	×	×	×	×
水平移位(像素)	2	2	2	2	2	2	2	2	×	×	×	×

5 结 论

本文对文本信息的内码进行 RS 纠错编码和冗余编码以增强鲁棒性,并对二值化后的内码进行随机置乱以增强安全性,充分利用 HVS 的屏蔽特性和一个改进的视觉模型计算图像分块的临界噪声阈值矩阵 JND,利用 Hilbert 扫描保持图像空间局部相关性的特点,不同强度地调整图像分块的 Hilbert 序列中两相邻分块小波变换后各对应细节子带均值之间的大小关系,以自适应地嵌入水印信号和确保盲水印提取,实现了文本信息以公开水印方式在图像中加密和解密的算法。实验结果表明,该算法的嵌入水印具有很好的透明性,并且对常见图像攻击有较高的鲁棒性,故该算法对保密通信是有效和实用的。

参考文献 (References)

1 Barni M, Bartolini F, Piva A. Improved wavelet-based watermarking

through pixel-wise masking [J]. IEEE Transactions on Image Processing, Greece 2001 ,10(5) :783 ~ 791.

2 Yang Heng-fu, Chen Xiao-wei. A robust image-adaptive public watermarking technique in wavelet domain [J]. Journal of Software, 2003, 14(9) :1652 ~ 1660. [杨恒伏, 陈孝威. 小波域鲁棒自适应公开水印技术 [J]. 软件学报, 2003, 14(9) :1652 ~ 1660.]

3 Cao J G, Fowler J E, Younan N H. An image-adaptive watermark based on a redundant wavelet transform [A]. In: Proceedings of the IEEE International Conference on Image Processing [C], Thessaloniki, Greece 2001 : 277 ~ 280.

4 Wang Zhi-ming, Zhang Yu-jin, Wu Jian-hua. A wavelet domain watermarking technique based on human visual system [J]. Journal of Nanchang University (Natural Science), 2005, 29(4) : 400 ~ 403. [王志明, 章毓晋, 吴建华. 一种改进的利用人眼视觉特性的小波域数字水印技术 [J]. 南昌大学学报 (理科版), 2005, 29(4) : 400 ~ 403.]

5 Sun Qiu-dong. An adaptive algorithm for edge detection based on visual perception model [J]. Journal of Shanghai Second Polytechnic University, 1998, 15(2) :83 ~ 90. [孙秋冬. 基于视觉模型的自适应图象边缘检测. 上海第二工业大学学报, 1998, 15(2) : 83 ~ 90.]